WHAT IS CLAIMED IS:

1. A method for securing management frames, the method comprising the steps of:

establishing an authenticated relationship between a transmitter and a receiver on a network;

generating a key;

deriving an information element based upon the key for signing a management frame packet transmitted on the network;

embedding the information element into the management frame packet;

transmitting the management frame packet to the receiver;

receiving the management frame packet; and

validating the information element in the received management frame packet.

2. The method set forth in claim 1 wherein the information element includes a message integrity check information element.

3. The method set forth in claim 1 further comprising the steps of:

generating a replay protection value for signing the management frame packet; and

adding the replay protection value into the management frame packet prior to transmitting.

4. The method set forth in claim 3 further comprising the step of validating the replay protection value.

5. The method set forth in claim 1 wherein the step of generating a key is concurrent with the step of establishing an authenticated relationship.

6. The method set forth in claim 1 wherein the step of establishing an authenticated relationship further includes employing a key establishment protocol.

7. The method set forth in claim 1 wherein the step of validating the information element further comprises the step of comparing the information element with a locally derived information element established by the receiver.

8. The method set forth in claim 2 wherein the step of validating the information element further comprises the step of comparing the message integrity check information element of the received management frame packet with a locally derived message integrity check information element established by the receiver.

9. The method set forth in claim 3 wherein the step of validating the information element further comprises the step of comparing the replay protection value of the received management frame packet with a locally derived replay protection value established by the receiver.

10. The method set forth in claim 1 wherein the receiver includes an access point.

11. The method set forth in claim 1 wherein the transmitter includes a wireless client.

12. The method set forth in claim 2 further comprising the step of generating the message integrity check value for the management frame packet prior to transmitting.

13. A system for securing a management frame packet, the system comprising: means for authenticating a relationship between a transmitter and a

receiver;

means for generating an information element for signing the management frame packet transmitted between the transmitter and the receiver via a network;

means for adding the information element into the management frame packet;

means for transmitting the management frame packet to the receiver via the network;

means for receiving the management frame packet; and

means for validating the information element in the received management frame packet.

14. The system set forth in claim 13 wherein the information element includes a message integrity check information element.

15. The system set forth in claim 14 wherein the information element further includes a replay protection value.

16. The system set forth in claim 13 wherein the means for transmitting the management frame packet is an IEEE 802.11 protocol.

17. The system set forth in claim 13 wherein the means for adding includes means for embedding the information element into a header of the management frame packet.

18. The method set forth in claim 14, wherein the message integrity check information element uniquely identifies the management frame communication to the authenticator.

19. A method for preventing IEEE 802.11 session disruption on a network,

comprising the steps of:

establishing a communication link between an access point and a wireless client on the network;

creating a trust relationship between the access point and the wireless client such that the wireless client adapted to securely access the network;

establishing a client-specific key for signing a management frame packet configured to be transmitted between the access point and the wireless client;

generating a message integrity check value based upon the client-specific key;

calculating a replay protection value for signing the management frame packet;

embedding the message integrity check value and the replay protection value into a header of the management frame packet;

transmitting the header to the access point; and

authenticating the header.

20. The method set forth in claim 19 further including the step, concurrent with the step of transmitting the header, transmitting the management frame packet.

21. The method set forth in claim 19 wherein a handshake protocol is utilized between the access point and the wireless client in the step of creating a trust relationship.

22. The method set forth in claim 19 wherein the step of authenticating further comprises the steps of:

calculating a local replay protection value;

generating a local message integrity check value;

comparing the received replay protection value with the local replay protection value; and

comparing the received message integrity check value with the local message integrity check value.

22. An article of manufacture embodied in a computer-readable medium for use in a processing system for authenticating management frame packets communicated to and/or from a network, the article comprising:

an authentication logic for causing the processing system to create a trusted relationship between a transmitter and a receiver;

a key generation logic for causing the processing system to generate a secure key for encrypting and signing an electronic management frame packet transmitted on the network;

a message integrity check generation logic for causing the processing system to generate a message integrity check for signing the electronic management frame packet transmitted on the network;

a replay protection value generation logic for causing the processing system to generate a replay protection value for signing the electronic management frame packet transmitted on the network;

a signing logic for causing the processing system to embed the message integrity check and the replay protection value into a header of the management frame packet;

a data transmitting logic for causing the processing system to transmit the header and the electronic management frame packet via the network; and

a message receiving logic for causing the processing system to verify the received message integrity check and the replay protection value included in the header.

23. The article as set forth in claim 22 wherein the data transmitting logic includes an IEEE 802.11 protocol.

24. The article as set forth in claim 22 wherein the replay protection value generation logic includes a sequential counter.

25. The article as set forth in claim 22 wherein the message receiving logic further includes logic for causing a processing system to compare a received message integrity check with a locally generated message integrity check.

26. The article as set forth in claim 22 wherein the message received logic further includes logic for causing a processing system to compare a received reply protection value with a locally calculated replay protection value.